

Response to Office Action
Docket No. 002.0230.US.UTL

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (currently amended): A system for providing a framework for
2 network appliance management in a distributed computing environment,
3 comprising:
4 an appliance status table recording a status report periodically received
5 from a status daemon autonomously operating on each of a plurality of network
6 appliances, each status report containing health and status information and
7 application-specific data ~~[[for]]~~ pertaining to autonomous configuration and
8 management of the each network appliance; and
9 a catalog server maintaining configuration settings for each network
10 appliance progressively assembled concurrent to providing installable
11 components and dynamically providing a catalog listing currently installable
12 components for each network appliance based on the configuration settings
13 independently received from the network appliance.
- 1 2. (original): A system according to Claim 1, further comprising:
2 a network operations center establishing a secure session with each
3 network appliance.
- 1 3. (original): A system according to Claim 1, further comprising:
2 a network operations center installing an initial set of installable
3 components on each network appliance during a bootstrap configuration.
- 1 4. (original): A system according to Claim 1, wherein the currently
2 installable components comprise at least one self-installable package, further
3 comprising:

Response to Office Action
Docket No. 002.0230.US.UTL

4 a component server supplying the at least one package for installation
5 responsive to a request from one such network appliance.

1 5. (original): A system according to Claim 4, further comprising:
2 a crypto module digitally signing the at least one package for the network
3 operations center prior to being supplied for installation.

1 6. (original): A system according to Claim 4, further comprising:
2 a crypto module encrypting the at least one package prior to being
3 supplied for installation.

1 7. (original): A system according to Claim 1, wherein the installable
2 components comprise at least one file, further comprising:
3 a component server supplying the at least one file responsive to a request
4 from one such network appliance.

1 8. (original): A system according to Claim 7, wherein the component
2 server establishes a secure session prior to the at least one file being supplied for
3 installation.

1 9. (original): A system according to Claim 7, further comprising:
2 a file information subdirectory specifying installation instructions for the
3 at least one file in a pre-determined entry prior to the at least one file being
4 supplied for installation.

1 10. (original): A system according to Claim 1, further comprising:
2 a proxy component server staging the currently installable components for
3 retrieval in a separate components database.

1 11. (original): A system according to Claim 1, wherein the distributed
2 computing environment is TCP/IP-compliant.

Response to Office Action
Docket No. 002.0230.US.UTL

1 12. (currently amended): A method for providing a framework for
2 network appliance management in a distributed computing environment,
3 comprising:
4 recording a status report periodically received from a status daemon
5 autonomously operating on each of a plurality of network appliances, each status
6 report containing health and status information and application-specific data
7 [[for]] pertaining to autonomously configuration and management of the each
8 network appliance;
9 maintaining configuration settings for each network appliance
10 progressively assembled concurrent to providing installable components; and
11 dynamically providing a catalog listing currently installable components
12 for each network appliance based on the configuration settings independently
13 received from the network appliance.

1 13. (original): A method according to Claim 12, further comprising:
2 establishing a secure session with each network appliance.

1 14. (original): A method according to Claim 12, further comprising:
2 installing an initial set of installable components on each network
3 appliance during a bootstrap configuration.

1 15. (original): A method according to Claim 12, wherein the currently
2 installable components comprise at least one self-installable package, further
3 comprising:
4 supplying the at least one package for installation responsive to a request
5 from one such network appliance.

1 16. (original): A method according to Claim 15, further comprising:
2 digitally signing the at least one package prior to being supplied for
3 installation.

1 17. (original): A method according to Claim 15, further comprising:

Response to Office Action
Docket No. 002.0230.US.UTL

2 encrypting the at least one package prior to being supplied for installation.

1 18. (original): A method according to Claim 12, wherein the installable
2 components comprise at least one file, further comprising:
3 supplying the at least one file responsive to a request from one such
4 network appliance.

1 19. (original): A method according to Claim 18, further comprising:
2 establishing a secure session prior to the at least one file being supplied for
3 installation.

1 20. (original): A method according to Claim 18, further comprising:
2 specifying installation instructions for the at least one file in a pre-
3 determined entry prior to the at least one file being supplied for installation.

1 21. (original): A method according to Claim 12, further comprising:
2 staging the currently installable components for retrieval in a separate
3 components database.

1 22. (original): A method according to Claim 12, wherein the
2 distributed computing environment is TCP/IP-compliant.

1 23. (original): A computer-readable storage medium holding code for
2 performing the method according to Claims 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,
3 or 22.

1 24. (currently amended): A system for autonomously managing a
2 network appliance deployed within a distributed computing environment,
3 comprising:
4 an internal catalog of components installed on one such network appliance
5 identified by component and version; and
6 a status daemon operating autonomously on the one such network
7 appliance and periodically providing a status report containing health and status

Response to Office Action
Docket No. 002.0230.US.UTL

8 information and application-specific data ~~[[fer]]~~ pertaining to autonomous
9 configuration and management of the one such network appliance; and
10 a catalog checker obtaining a catalog of currently installable components
11 dynamically generated for the one such network appliance based on the status
12 report independently received from the one such network appliance and
13 determining non-current components by comparing the components and versions
14 listed in the obtained catalog against the internal catalog.

1 25. (original): A system according to Claim 24, further comprising:
2 a network operations center negotiating a secure connection with the one
3 such network appliance.

1 26. (original): A system according to Claim 24, further comprising:
2 an initial plug-in executed on the one such network appliance.

1 27. (original): A system according to Claim 24, further comprising:
2 a post plug-in executed on the one such network appliance.

1 28. (original): A system according to Claim 24, further comprising:
2 a network operations center broadcasting a query message to each such
3 network appliance to trigger a status report.

1 29. (original): A system according to Claim 24, wherein the
2 components comprise at least one self-installable package, further comprising:
3 an installer obtaining the at least one self-installable package and installing
4 the at least one self-installable package per instructions encoded therein.

1 30. (original): A system according to Claim 29, wherein the
2 components further comprise at least one file dependent on the at least one self-
3 installable package, further comprising:
4 an installer obtaining the at least one file subsequent to installing the at
5 least one self-installable package and installing the at least one self-installable
6 package per instructions stored in a pre-determined entry.

Response to Office Action
Docket No. 002.0230.US.UTL

1 31. (original): A system according to Claim 29, further comprising:
2 a component server negotiating a non-secure session prior to obtaining the
3 at least one self-installable package.

1 32. (original): A system according to Claim 29, further comprising:
2 a crypto module at least one of authenticating and decrypting the at least
3 one self-installable package prior to installing the at least one self-installable
4 package.

1 33. (original): A system according to Claim 29, wherein the
2 instructions comprise an executable installation program plus one or more files to
3 be installed.

1 34. (original): A system according to Claim 29, wherein the
2 components further comprise at least one file, further comprising:
3 an installer obtaining the at least one file and installing the at least one
4 self-installable package per instructions stored in a pre-determined entry.

1 35. (original): A system according to Claim 34, further comprising:
2 a component server negotiating a secure session prior to obtaining the at
3 least one self-installable package.

1 36. (original): A system according to Claim 34, wherein the pre-
2 determined entry comprise a file information subdirectory identifying installation
3 instructions.

1 37. (original): A system according to Claim 29, wherein at least one
2 such network appliance performs one of electronic mail anti-virus scanning,
3 content filtering, packet routing, and file, Web and print servicing.

1 38. (original): A system according to Claim 29, wherein the distributed
2 computing environment is TCP/IP-compliant.

Response to Office Action
Docket No. 002.0230.US.UTL

- 1 39. (currently amended): A method for autonomously managing a
2 network appliance deployed within a distributed computing environment,
3 comprising:
4 maintaining an internal catalog of components installed on one such
5 network appliance identified by component and version;
6 periodically providing a status report containing health and status
7 information and application-specific data ~~[[fe]]~~ pertaining to autonomous
8 configuration and management of the one such network appliance and received
9 from a status daemon autonomously operating on for the one such network
10 appliance;
11 obtaining a catalog of currently installable components dynamically
12 generated for the one such network appliance based on the status report
13 independently received from the one such network appliance; and
14 determining non-current components by comparing the components and
15 versions listed in the obtained catalog against the internal catalog.
- 1 40. (original): A method according to Claim 39, further comprising:
2 negotiating a secure connection with the one such network appliance.
- 1 41. (original): A method according to Claim 39, further comprising:
2 executing an initial plug-in on the one such network appliance.
- 1 42. (original): A method according to Claim 39, further comprising:
2 executing a post plug-in on the one such network appliance.
- 1 43. (original): A method according to Claim 39, further comprising:
2 broadcasting a query message to each such network appliance to trigger a
3 status report.
- 1 44. (original): A method according to Claim 39, wherein the
2 components comprise at least one self-installable package, further comprising:
3 obtaining the at least one self-installable package; and

Response to Office Action
Docket No. 002.0230.US.UTL

4 installing the at least one self-installable package per instructions encoded
5 therein.

1 45. (original): A method according to Claim 44, wherein the
2 components further comprise at least one file dependent on the at least one self-
3 installable package, further comprising:
4 obtaining the at least one file subsequent to installing the at least one self-
5 installable package; and
6 installing the at least one self-installable package per instructions stored in
7 a pre-determined entry.

1 46. (original): A method according to Claim 44, further comprising:
2 negotiating a non-secure session prior to obtaining the at least one self-
3 installable package.

1 47. (original): A method according to Claim 44, further comprising:
2 at least one of authenticating and decrypting the at least one self-
3 installable package prior to installing the at least one self-installable package.

1 48. (original): A method according to Claim 44, wherein the
2 instructions comprise an executable installation program plus one or more files to
3 be installed.

1 49. (original): A method according to Claim 39, wherein the
2 components further comprise at least one file, further comprising:
3 obtaining the at least one file; and
4 installing the at least one self-installable package per instructions stored in
5 a pre-determined entry.

1 50. (original): A method according to Claim 49, further comprising:
2 negotiating a secure session prior to obtaining the at least one self-
3 installable package.

Response to Office Action
Docket No. 002.0230.US.UTL

1 51. (original): A method according to Claim 49, wherein the pre-
2 determined entry comprise a file information subdirectory identifying installation
3 instructions.

1 52. (original): A method according to Claim 39, wherein at least one
2 such network appliance performs one of electronic mail anti-virus scanning,
3 content filtering, packet routing, and file, Web and print servicing.

1 53. (original): A method according to Claim 39, wherein the
2 distributed computing environment is TCP/IP-compliant.

1 54. (original): A computer-readable storage medium holding code for
2 performing the method according to Claims 39, 40, 41, 42, 43, 44, 45, 46, 47, 48,
3 49, 50, 51, 52, or 53.